A New Watermarking Algorithm Based on Image Scrambling and SVD in the Wavelet Domain

U. M. Gokhale[1], Y. V. Joshi[2]

[1] U.M.Gokhale is working as Asst.Professor in Electronics and Telecommunication Department in G.H.Raisoni Institute of Engineering and Technology for Women, Nagpur., Maharashtra, India
(e-mail : umgokhale@gmail.com)

[2] Y.V.Joshi is working as Director Walchand College Of Engineering Sangli, Maharashtra, India
(e-mail:yashwant.josh@gmail.com).

***Abstract*- A new watermarking algorithm which is based on image scrambling and SVD in the wavelet domain is discussed in this paper. In the proposed algorithm, chaotic signals are generated using logistic mapping and are used for scrambling the original watermark. The initial values of logistic mapping are taken as private keys. The covert image is decomposed into four bands using integer wavelet transform; we apply SVD to each band and embed the scrambled watermark data by modifying the singular values.**

***Index words* - logistic mapping, singular value decomposition, discrete wavelet transforms.**

I. INTRODUCTION

With the rapid growth of internet and networks techniques, Multimedia data transforming and sharing has become common to many people. Multimedia data is easily copied and modified, so necessity for copyright protection is increasing. Digital watermarking has been proposed as the technique for copyright protection of multimedia data. Existing watermarking schemes can be divided into two categories spatial domain and transform domain. Spatial domain techniques embed data by directly modifying pixel values of the host image, while transform domain techniques embed data by modifying transform domain coefficients. Discrete cosine transform (DCT) and discrete wavelet transform (DWT), which are used in image compression standards JPEG and JPEG2000 respectively , are two main transform methods used in transform domain watermarking. However, transform methods attempt to decompose images in terms of a standard basis set. This is not necessarily the optimum set. Recently Singular value decomposition (SVD) has been used for implementation of watermarking algorithms [1-10].

II. THE RELATED WORK

In [1] Gorodetski et al. embed watermark bits by modifying the quantized singular values of the host image. In [2], Chandra computed SVD of both the host and watermark images and then singular values of the watermark images are minified and added to those of the host image. In [3] Liu and Tan applied SVD to only host image and watermark bits are directly added to its singular values. In [4] Ganic et al. Propose a two layer watermarking scheme. In [5] SVD is used with DCT and in [6] SVD is used with DWT embedding data in all frequencies. In [7] Agrawal et al. Propose a scheme of modifying the singular vectors instead of singular values. In [8] Ghazy et al. Proposed a scheme in which the image is divided into blocks and then watermark is embedded in singular values of each block separately. In [9] SVD is used with a human visual system (HVS) model. In [11] , however, it is demonstrated that a counterfeit attack on SVD watermarked image is possible and proposes a method to counterattack it. In [12] and [13] it is pointed out that SVD watermarking suffers from false watermark detection. In [14] it has been shown that SVD based watermarking algorithms are robust to distortions as long as attacks are not severe, also an attack method to extract a false watermark from any watermarked image is proposed. Thus SVD based watermarking methods cannot be used for the ownership of an image. In our proposed scheme watermarking is used for image authentication.

III. SINGULAR VALUE DECOMPOSITION AND IMAGE ENCRYPTION

A. Singular Value Decomposition

Let A be an image matrix of size N×N. Using SVD the matrix A can be decomposed as:

$$A = U_A S_A V_A^T = \sum_{i=1}^{r} u_i \; s_i \, v_i^T \tag{1}$$

With

$$U_A = [u_1 , u_2 , \dots u_N] \tag{2}$$

$$V_A = [v_1 , v_2 , \dots v_N] \tag{3}$$

$$S_A = \begin{bmatrix} s_1 & 0 & \cdots 0 \\ 0 & s_2 & \cdots 0 \\ \vdots & \vdots & \ddots \quad \vdots \\ 0 & 0 \cdots & s_N \end{bmatrix} \tag{4}$$

Where r is the rank of matrix A(r d” N), UA and V_A are orthogonal matrices of size N×N, whose column vectors are u_i and v_i. S is an N×N diagonal matrix containing the singular values s_i assumed to be in decreasing order.

DOI: 01.IJNS.02.03.141

In watermarking applications, SVD has following properties:
1) SVD is able to efficiently represent the intrinsic algebraic properties of an image, where singular values correspond to the luminance of the image and singular vectors reflect geometry characteristics of the image.
2) Singular values have good stability, which means small perturbation added to image will not significantly change the corresponding singular values.
3) An image matrix has many small singular values compared with the first value. If these values are ignored it will have much effect on the quality of reconstructed image.

B. Image Encryption

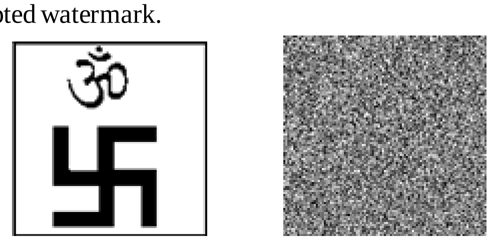
Chaos signal are a kind of pseudorandom, irreversible and dynamical signals generated by deterministic non linear equations, which possess good characteristics of pseudorandom sequences. There are many ways to generate chaos sequence. We apply logistic mapping chaos sequence. The equation for logistic mapping chaos is given by equation (5).

$$X(n+1) = \mu X(n)\left(1 - X(n)\right) \qquad (5)$$

Where 0 d" µ d" 4, is called as branch parameter, x õ(0,1).Logistic map is chaotic when 3.569945d" µ d" 4,chaotic systems are highly sensitive to initial parameters. In order to get chaotic sequence, the chaotic signal x (n+1) must be transformed into binary sequences. We use the logistic map to generate sequence W (i). Then, we set a threshold T. If element of sequence is larger than the threshold, we replace that element by 1; otherwise, replace by 0, as described by equation (6).

$$W(i) = \begin{cases} 1, & W_i > T \\ 0, & W_i < T \end{cases} \qquad (6)$$

Make the xor operation between the sequence and the matrix of the original watermark to obtain the scrambled watermark or encrypted watermark. Fig 1 shows the original and the encrypted watermark.



IV. PROPOSED METHOD

Proposed method is explained in the following section. The scrambled watermark is obtained from the original watermark and is embedded into the cover image. The watermarked image is distributed. When required the test image is checked for the presence of the watermark by the watermark detection algorithm. As the watermark is semi fragile it allows to alter the image by specific image processing operations.

A. Watermark embedding:

The watermark embedding algorithm is as follows:
1) Using the integer wavelet transform(IWT), cover image A is first decomposed into four sub bands LL,HL,LH,HH as shown in Fig.2.

$$A \rightarrow I_s \;\; (s \in (LL, HL, LH, HH) \qquad (7)$$

2) Apply SVD to each sub band image :

$$I_s \rightarrow U_s S_s V_s^T \qquad (8)$$

3) Obtain the scrambled or encrypted image from the original image by using logistic mapping as described in section 2.

$$W = W(i) xor\ K \qquad (9)$$

4) Apply SVD to the encrypted image.

$$W \rightarrow U_w S_w V_w^T \qquad (10)$$

5) Modify the singular values of the cover image in each sub band with singular values of the encrypted watermark;

$$\hat{I_s} \rightarrow U_s\,(S_s + \alpha S_w) V_s^T \qquad (11)$$

6) Obtain the four sets of modified IWT coefficients.

7) Apply the inverse IWT using the four sets of modified IWT coefficients to produce the watermarked cover image.

$$\hat{A} \leftarrow \hat{I_s} \qquad (12)$$

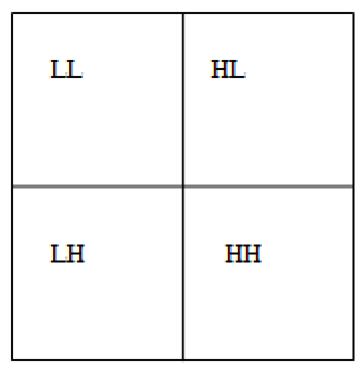


Figure 2 Wavelet decomposition

B. Watermark detection

The watermark detection algorithm is as follows
1)Using DWT, decompose the watermarked (and possibly attacked) cover image Â into four sub bands LL, HL, LH, HH as shown in Fig 2.

$$\hat{A} \rightarrow \hat{I}_s \;\; (s \in \; LL, HL, LH, HH) \qquad (13)$$

2) Apply SVD to each sub band image :

$$\hat{I}_s \rightarrow \hat{U}_s \hat{S}_s \hat{V}_s^T \qquad (14)$$

3) Extract the singular values from each sub band

$$\hat{S}_{ws} \leftarrow \frac{\hat{S}_s - S_s}{\alpha} \qquad (15)$$

DOI: 01.IJNS.02.03.141

1) Construct four watermark images from four sub bands.

$$W_s \rightarrow U_w \hat{S}_{ws} V_w^T \quad (16)$$

2) The original watermark can be obtained by xor operation with the chaotic sequence W (i).

$$K_s = W(i)\, xor\, W_s \quad (17)$$

V. EXPERIMENTAL RESULTS

The experimental simulation is carried out using MATLAB. The standard test images of 512×512×8 greyscale were used for studying the effects of perceptibility and robustness of the watermarking algorithm on a 256 × 256 binary watermark image. In order to evaluate the difference between cover image and watermarked image, we used Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) to estimate the watermark imperceptibility.

$$PSNR = 10log10\left(\frac{255 * 255}{MSE}\right) \quad (18)$$

Where, MSE is the Mean Square Error between the original and watermarked image.

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{i=0}^{N-1}[\{x(i,j) - y(i,j)\}^2] \quad (19)$$

Where x (i, j) and y (i, j) represent the pixel value of the original and the watermarked image respectively. A higher PSNR indicates that the quality of the watermarked image is closer to the original image. Fig 2 shows the original and watermarked image. We estimate the similarity between the original watermark and the extracted watermark using normalized correlation (NC):

$$NC = \frac{\sum_{i=1}^{L} w(i) \times \hat{w}(i)}{\sqrt{\sum_{i=1}^{L} w(i)^2}\sqrt{\sum_{i=1}^{L} \hat{w}(i)^2}} \quad (20)$$

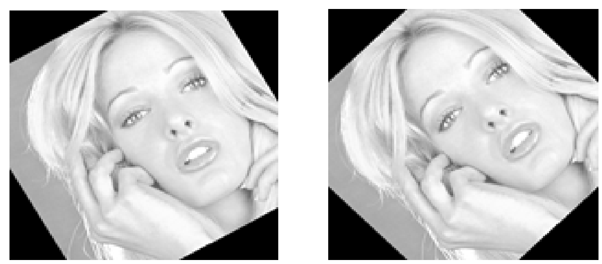
The NC shows the robustness of the algorithm. Its value is 1.0000 before the watermark image is attacked. The results for different attacks are shown in table I. In order to investigate robustness watermarked image was attacked by various attacks. The original image is shown in Figure 3(a), and the watermarked image is shown in Figure 3(b). Fig 4 shows the salt and pepper noise attack. Fig 5 shows Gaussian noise attack and Fig 6 show the rotation attack. Table I-IV shows the results for the various attacks and their effects on PSNR, NC and extracted watermark.

Figure 3 a) Original image b) Watermarked image

Figure 4 Watermarked image after adding salt pepper noise

a) Variance =0.001 b) variance = 0.002

Figure 5 after adding Gaussian noise



a) 30^0 b) 45^0

Figure 6 Wwatermarked image after Rotation

TABLE II PSNR AND NC FOR GAUSSIAN NOISE ATTACK

Gaussian variance	PSNR(dB)	NC
0.001	26.41	1.0000
0.002	25.19	0.9991
0.003	24.27	0.9954
0.004	23.52	0.9890
0.005	22.90	0.9817

TABLE III PSNR AND NC FOR SALT AND PEPPER NOISE ATTACK

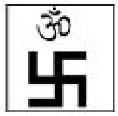
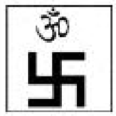
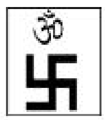
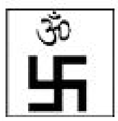
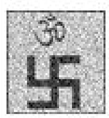
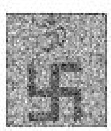
Salt & Pepper noise	PSNR(dB)	NC
0.005	24.60	1.0000
0.01	22.81	0.9999
0.02	20.47	0.9974
0.04	17.94	0.9875
0.10	14.18	0.9621

TABLE IV PSNR AND NC FOR ROTATION ATTACK

Rotation	PSNR (dB)	NC
5^o	14.44	0.8312
10^o	12.23	0.8017
15^o	11.04	0.7877
30^o	9.39	0.7569
45^o	8.96	0.7287

DOI: 01.IJNS.02.03.141

TABLE I VARIOUS ATTACKS AND THEIR EFFECT

Attack	PSNR (dB) Before	PSNR (db) After	NC	Extracted Watermark
Salt & pepper (0.01)	52.46	22.81	0.9999	
Salt & pepper (0.02)	52.46	20.47	0.9974	
Gaussian Noise (0,0.001)	52.46	26.41	1.0000	
Gaussian Noise (0,0.002)	52.46	25.92	0.9991	
Rotation 30^0	52.46	9.39	0.7569	
Rotation 45^0	52.46	8.96	0.7287	

VI. CONCLUSIONS

The proposed watermarking algorithm is *non-blind* watermarking technique as the original image is required for the watermark extraction. The PSNR is 52.46 before the attacks. The value of NC is close to 1.0000 which shows the robustness to the attack. In the existing watermarking algorithms there is always a trade off between higher robustness and degree of perceptibility. The proposed algorithm achieves both high robustness and imperceptibility. The security of the watermark is improved by its encryption using the chaos sequence generated by logistic mapping. Thus it can be used for image authentication.

REFERENCES

1. V.Gorodetski, L. Popyack, V. Samoilov and V. Skormin, " SVD based approach to transparent embedding data into digital images," in proc. International Workshop on mathematical methods, model and architectures for computer network security (MMM-ACNS'01), may 2001

2. Chandra D.V.S.; "Digital image watermarking using singular value decomposition", Circuits and Systems 2002.MWSCAS-2002, vol.3, 4-7Aug 2002, pp. 264-267.

3. R. Liu, T. Tan, "An SVD –based watermarking scheme for protecting rightful ownership", *IEEE Transaction on* Multimedia Volume 4, issue 1, March 2002 pp121-128.

4. E.Gagnic, N. Zubair and A.M.Eskicioglu, "An optimal Watermarking based on singular value decomposition,"in proc *IASTED international Conference on Communication , network and Information security(CNIS'03),*Dec.2003

5. A.Sverdlov, S. Dexter and A.M.Eskicioglu, "Robust DCT-SVD domain image watermarking for copyright protection : Embedding data in all frequencies, in proc. the 2004 Multimedia and Security Workshop, ACM press, sep 2004,pp. 166-174.

6. E. Gagnic and A.M. Eskicioglu, "Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition", Journal of Electronic Imaging vol. 14, no.4, Dec 2005.

7. R.Agrawal and M.S.Santhanam, "Digital watermarking in the singular vector domain,"Mar.2006.

8. R.A.Ghazy, N.A El-Fishawy, M. M Hadhoud, M.I.Dessouky and F.E. Abd El-Samie, "An efficient Block by block SVD based image watermarking scheme", Ubiquitous computing and communication Journal ,2(5),2007,pp. 1-9.

9. Q.Li, C. Yuan and Y.Z. Zhong, "A novel SVD based watermarking scheme using human visual model," in Proc. The 2nd International Symposium on Computational intelligence and Industrial Applications, Nov 2006.

10. Andrews H, Patterson C., "Singular Value Decomposition (SVD) Image Coding", *IEEE Transaction on [legacy, pre-1988], Volume 24, Issue 4, April 1976, pp425-432*.

11. Y.D.Wu, "On the security of an SVD-Based Ownership Watermarking, IEEE Transactions on Multimedia, 7 (4), August 2005, pp.624-627

DOI: 01.IJNS.02.03.141

12. X.P. Zhang, K.Li comments on "An SVD-Based Watermarking scheme for Protecting Rightful Ownership", IEEE Transaction on multimedia Vol.7,no.2,2005, pp.593-594.
13. R.Rykaczewski, comments on "An SVD-Based Watermarking scheme for Protecting Rightful Ownership", IEEE Transaction on multimedia Vol.9,no.2,2007,pp.421-423.
14. Xiong Changzhen, Guo Fenhong,Li Zhengxi, "Weakness Analysis of Singular Value based Watermarking", in proceedings of the 2009 IEEE international Conference on Mechtronics and Automation August 9-12, Changchun, China.

U.M Gokhale is presently working as Asst.Professor and Head in Department of Electronics and Telecommunication in G.H.Raisoni Institute of Engineering and Technology for women, Nagpur (MS), India. He is Life member of Indian Society for Technical Education (ISTE) and also Associate member of Institution of Engineers (IE).He has 22 years teaching experience in Engineering College.

Dr. Y. V. Joshi is presently working as Director of Walchand College of Engineering, Sangli since May 2009. Earlier he was at SGGS Institute of Engineering and Technology, Vishnupuri, Nanded since 1986 in various capacities starting with Lecturer (1986-1993), Assistant Professor (1993-2001), Professor (2001 onwards). He also served as Head of Electronics and Telecommunication Engineering department (2002-04), First Dean of Academics (2004-06), Dean (Finance and Resource Mobilization (2007-08). He did his graduation B. E. Electronics in 1986 and post graduation M. E. Electronics 1991 from SGGS Institute of Engineering and Technology, Vishnupuri, Nanded. He completed Ph. D. (1998) from IIT, Delhi. He has 15 international Journal publications and 25 national and international conference publications to his credit. He is Life Member of ISTE. He conducts and supervises research in the areas of Signal and Image processing.He has so far supervised more than 25 M.E./M. Tech dissertations and 3 Ph. D. students.

DOI: 01.IJNS.02.03.141